WHAT IS CLAIMED IS:

1. A method for intercepting a command sent to a manager program generated by a client program and determining whether said command is characteristic of a normal application program, the method comprising the steps of:

intercepting said command;

preventing the direct sending of said command from said client program to said manager program;

performing an analysis upon said command;

sending said command to said manager program if said analysis determines that said command is characteristic of a normal application program; and

preventing said command from reaching said manager program if said analysis determines that said command is not characteristic of a normal application program;

whereby said manager program is protected from commands that are sent from a client program that is under control of an attacker.

2. The method of claim 1, further comprising the step of:

permanently storing said command.

3. The method of claim 1, further comprising:

alerting an administrator through a notification channel if said analysis determines that said command is not characteristic of a normal application program.

4. The method of claim 1, further comprising:

storing normal patterns that correspond to commands generated by said normal application programs;

said analyzing step comprises:

determining whether said command corresponds to any of said stored patterns, and

determining whether said command is characteristic of a normal application program if said analysis determines that said command corresponds to any of said stored patterns.

5. The method of claim 1, further comprising:

storing attacker patterns that correspond to commands generated by a client program that is under control of an attacker,

said analyzing step comprises:

determining whether said command corresponds to said stored attacker patterns, and

determining that said command is not characteristic of a normal application program if said analysis determines that said command corresponds to any of said attacker patterns.

6. The method of claim 1, wherein:

said manager program is a database manager.

7. The method of claim 6, wherein:

said command is a Structured Query Language query.

8. An application firewall program for intercepting a command sent from a client program to a manager program and determining whether said command is characteristic of a normal application program, comprising:

a preventor step to prevent the direct sending of said command from said client program to said manager program;

an analysis step whereby said command is analyzed to determine if it is characteristic of a normal application program; and

a forwarding step in which said command is sent to said manager program provided said analysis determines that said command is characteristic of a normal program; and

a prevention step in which commands that are not characteristic of a normal application program are prevented from reaching said manager program.

9. The application firewall program of claim 8 further comprising:

data storage.

10. An application firewall machine comprising:

a first network interface coupling said firewall machine to a client computer via a first network segment;

a second network interface coupling said firewall machine to a manager computer via a second network segment;

a communications manager coupled to said first and second network interfaces, said communications manager being operable to read and write data to said first and second network segments via the corresponding first and second network interfaces, said communications manager being further operable to not permit direct passage of network

communications across the network interfaces, and operable to send data to said manager computer when analysis determines that data coming from said client computer contains a command that is characteristic of a normal program; and

a command processor to process said data to identify commands that are being passed as requests from said client computer to said manager computer, and

a command analyzer to analyze said commands to determine if said commands are characteristic of a normal application program.

11. An application firewall machine in accordance with claim 10 wherein:

said client machine comprises a database client program, said database client program being operable to generate commands that are directed to said manager machine; and

said manager machine comprises a database manager program, said database manager program receiving commands sent by said client machine.

12. An application firewall machine in accordance with claim 11 wherein:

said commands are SQL commands;

said client machine comprises a database client program generating said SQL commands directed to said manager machine; and

said manager machine comprises a database manager program capable of receiving said SQL commands.

13. An application firewall machine in accordance with claim 10 further comprising:

a data storage manager.

14. An application firewall machine in accordance with claim 13 wherein:

said storage manager comprise stored data representing invalid commands that said client computer should never generate and which are indicative of attack; and

said command analyzer utilizes said data representing invalid commands.

15. An application firewall machine in accordance with claim 13 wherein:

said storage manager comprise stored data which represents only normal commands that said client computer should generate; and

said command analyzer utilizes said stored data.

16. An application firewall machine in accordance with claim 13 wherein:

said storage manager comprises an SQL database manager.

17. An application firewall machine in accordance with claim 13 wherein:

said storage manager comprises an indexed file system storage.

18. An application firewall machine in accordance with claim 13 wherein:

said storage manager comprises a file system storage.

19. An application firewall machine in accordance with claim 13 wherein:

said storage manager comprises distributed file system storage.

20. An application firewall machine in accordance with claim 10, further comprising:

an alerting interface operable to alerts an administrator through a notification channel, if said analysis determines that said command is not characteristic of a normal application program;

whereby the alert allows the administrator to initiate a course of action that further protects said manager. if said analysis determines that said command is not characteristic of a normal application program, said alerting interface

21. An application firewall machine in accordance with claim 17 wherein:

said alerting interface may send information about said attack to a destination selected from the group consisting of an SMTP servers, SNMP managers, system log files, and wireless pager notification.

5